1. A tamper evident wireless application protocol identity module (WIM) including stored thereon a public-private key pair and a manufacturer certificate, wherein the certificate contains a set of fields holding data relating to said key pair, the certificate being signed using a further private key.

2. A module as claimed in Claim 1, wherein the public key is held within a field of said certificate.

3. A module as claimed in Claim 1 or Claim 2, further including a certification authority certificate.

4. A module as claimed in any preceding Claim, wherein the at least one certificate is stored externally of said module at a remote location which is derivable from an address stored on said module.

5. A module as claimed in any preceding Claim, wherein the further private key is the manufacturer's private key.

6. A module as claimed in any one of Claims 1 to 4, wherein the further private key is an initial management key, the module further having stored thereon an initial management certificate signed using the manufacturer's private key.

7. A method of manufacturing a tamper-evident wireless application protocol identity module (WIM) including the steps of storing a public-private key pair on said module together with a manufacturer certificate signed using a further private key.

8. A method according to Claim 7, wherein the key pair is created externally of said module.

9. A method according to Claim 7, wherein the key pair is created internally of said module.

10. A method according to Claim 8 or Claim 9, wherein the manufacturer certificate is created externally of the module.

11. A method according to Claim 10 as appendant to Claim 9, wherein the module is accessed to obtain the public key to facilitate the external creation of the certificate.

12. A method as claimed in any one of Claims 7 to 11, wherein the further private key is the manufacturer's private key.

13. A method as claimed in Claim 9, including the additional steps of: storing an externally created initial management key pair and an initial management certificate signed using the manufacturer's private key on said module, and storing an internally created manufacturer certificate on said module wherein the further private key is the initial management private key.

14. A method of validating a tamper-evident wireless application protocol identity module (WIM) on which is stored at least one public-private key pair together with a manufacturer certificate signed using a further private key, the method including the step of querying a public directory to obtain a public key certificate with which to verify the signature generated by the further private key.

15. A method of validating the identity of a communication terminal for conducting transactions on a network comprising establishing the identity of a user of the terminal connected to the network, interrogating the terminal to obtain a public key of a public-private key pair stored on the terminal, confirming the authenticity of a certificate signed by the module manufacturer supporting the public key and subsequently issuing a further certificate for the public key which certificate is available to support transactions with the terminal over the network.

16. A method as claimed in Claim 15, wherein the network service provider carries out the authentication of the manufacturer certificate.

17. A communications device having stored thereon a plurality of certificates supporting security operations including authentication and non-repudiation, and further including a manufacturer certificate stored on a tamper evident module, wherein the manufacturer certificate contains a set of fields holding data relating to a public-private key pair for application layer security, at least the private key being stored on said module, the manufacturer certificate being signed using a further private key.

18. A device as claimed in Claim 17, wherein at least one certificate supporting security operations is stored externally of said device at a remote location which is derivable from an address stored on said device.

19. A method of satisfying an identity module issuer of the provenance of an identity module for use in transactions on a network comprises the

issuer approving a manufacturing process of the module manufacturer, and having the manufacturer store a manufacturer certificate signed securely by the manufacturer on a module produced in accordance with the approved process, wherein on connection to the network of a terminal containing a module, the signature is verified to determine whether it is the manufacturer's.

20. A method as claimed in Claim 19, wherein the manufacturer certificate is signed using the manufacturer's private key such that on connection to the network a public key certificate is obtained with which verify the signature.

21. A method as claimed in Claim 19 or Claim 20, wherein the verification of the signature is carried out by the issuer.

22. A method as claimed in any one of Claims 19 to 21, wherein following successful verification of a signature, a further public key certificate is made available to support transactions with the terminal, the public key having been stored in the manufacturer certificate.